UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/989,261	12/12/97	PAONE	L 831-2

LM02/0316

CHARLES R HOFFMANN
HOFFMANN & BARON LLP
6900 JERICHO TURNPIKE
SYOSSET NY 11791

EXAMINER	
KABAKOFF,S	
ART UNIT	**PAPER NUMBER**
2767	7

DATE MAILED: 03/16/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	08/989,261	PAONE, LUCIANO F.	
	Examiner	Art Unit	
	Steve Kabakoff	2767	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☒ Responsive to communication(s) filed on *04 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) *25-29,33 and 35* is/are withdrawn from consideration.

5)☒ Claim(s) *9* is/are allowed.

6)☒ Claim(s) *1-8,10-20,30-32 and 34* is/are rejected.

7)☒ Claim(s) *21-24* is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

14) ☒ Notice of References Cited (PTO-892)
15) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
16) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
17) ☒ Interview Summary (PTO-413) Paper No(s). *7* .
18) ☐ Notice of Informal Patent Application (PTO-152)
19) ☐ Other: .

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-24, 30-32, and 34, drawn to a block encryption method, classified in class 380, subclass 28.

   II. Claims 25-29, 33, 35, drawn to digital signature authentication, classified in class 713, subclass 176.

2. During a telephone conversation with Glenn Henneberger on March 6, 2000 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-24, 30-32, and 34. Affirmation of this election must be made by applicant in replying to this Office action. Claims 25-29, 33, and 35 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

3. Claims 1-24, 30-32, and 34 have been examined.

Response to Arguments

4. The examiner withdraws the previous rejections of claims 1-24, 30-32, and 34 and acknowledges the telephone agreement made between Examiner Reba Elmore and Glenn Henneberger on December 22, 1999 such that Examiner Elmore promised to allow the instant application or have a non-final action issued.

Claim Objections

5. Claims 21-24 are objected to because of the following informalities:

The word "traverse" should be changed to "transverse" in line 7 of claim 21.

The word "arry" should be changed to "array" in line 20 of claim 21.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-5, 8, 16, 18, 19, 30-32, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (US 5003596) in view of Colvin, Sr (US 5841872).

As per claim 1, the claimed invention teaches encrypting input plaintext using an object key where the object key comprises data and methods. Wood (US 5003596) teaches a block encryption method to convert a block of input plaintext into a unique block of ciphertext (see column 3, lines 38-40 and Fig. 1). In the method of Wood (US 5003596), encryption keys are selected from a key table for use in the encryption process (column 3, lines 66-68). The block encryption method in Wood (US 5003596) differs from the block encryption method in claim 1 since the encryption keys in Wood (US 5003596) are not object keys as defined in claim 1.

The "object key comprising data and methods" in claim 1 is interpreted by the examiner to refer to an object associated with object-oriented programming (OOP). Anyone skilled in the art of computer science would know an *object* in OOP is composed of *data* (sometimes referred to as "attributes") and *methods*. Therefore, one skilled in the art would understand the object key in claim 1 to comprise methods designed to implement an encryption process and corresponding data to support the methods.

The examiner asserts that it is well known to implement encryption using OOP. In fact, encryption classes are ubiquitous in the art of programming in high level languages such as C++ and Java. It appears the examiner who wrote the first office action presented the Shanton (US 5369702) reference to illustrate an object-oriented encryption system, however Colvin, Sr (US 5841872) more explicitly shows a block encryption process implemented using an OOP encryption class.

In Colvin, Sr (US 5841872), column 4, lines 25-66 show a specific encryption class "DataSpin" comprising data (S, T, U, V, W, X, Y, and Z) and methods (SPIN_LEFT and SPIN_RIGHT). Column 5, lines 40-43 in Colvin, Sr (US 5841872) explain that the state variables in the disclosed encryption class are equivalent to an encryption key.

The applicant may assert the encryption key object in Colvin, Sr (US 5841872) does not implement the same block encryption method taught in the claimed inventions; this is correct. *The Colvin, Sr (US 5841872) reference is simply being used as evidence to show how an encryption key object containing data and methods, such as the object key in claim 1, is a very well known OOP encryption class implementation.*

Therefore, one of ordinary skill in the art of programming would know to code the encryption keys in Wood (US 5003596) using OOP to create an encryption key object similar to

that in Colvin, Sr (US 5841872). It would have been obvious to one of ordinary skill in the art at the time of the invention to create the encryption key in Wood (US 5003596) using OOP, as shown in Colvin, Sr (US 5841872), since OOP is well known in the art as a means for compact, modular, high-level coding of block encryption processes.

As per claim 2, the claimed invention limits claim 1 so the encryption process is a block cipher system. The encryption process disclosed in Wood (US 5003596) is also a block cipher system (column 3, lines 38-40 and Fig. 1).

As per claims 3 and 4, the claimed inventions limit claims 2 and 1 respectively so the encryption key changes with each block of data encrypted. The encryption key in Wood (US 5003596) also changes with every block of data encrypted (column 3, lines 38-40).

As per claim 5, the claimed invention limits claim 1 so the following the following is done before the step of encrypting:

(i) the user creates an initial state of the object

(ii) an initial state of a random session key is created

(iii) the initial state of the random session key is encrypted using the initial state of the object

(iv) the object key is modified based on seeding from the random session key before each input data block is encrypted to ensure each input data block is encrypted using a unique key

Step (i) is standard in OOP when an object's constructor is executed (in Colvin, Sr (US 5841872), the constructor is DataSpin::DataSpin). The method of Colvin, Sr (US 5841872) shows a typical constructor that initializes an encryption key (the eight state variables in class DataSpin).

Step (ii) is disclosed in column 6, lines 19-21 of Wood (US 5003596) since a random initializing vector is typically created to seed a key generating function (see column 9, lines 7-35 regarding the key generation function in Wood (US 5003596)).

Step (iii) is a well known step of encrypting a generated initializing vector using an initial encryption key as shown in reference number 36 in Fig. 2 of Wood (US 5003596) (see column 6, lines 25-34). The examiner notes the initializing vector in Wood (US 5003596) is tantamount to the random session key in claim 5, and the initial key in Wood (US 5003596) is equivalent to the initial state of the object in claim 5.

Step (iv) is disclosed in column 3, line 68 through column 4, line 6 in Wood (US 5003596) since the encryption object key in the method taught in Wood (US 5003596) is modified for every block of plaintext encrypted. The encryption object key in the method of Wood (US 5003596) is modified by selecting a new key from a key schedule and replacing the old encryption key, where the key selection process depends on an initializing vector and the current state of the plaintext, ciphertext, and associated mask values.

As per claim 8, the claimed invention limits claim 5 so each object key is associated with its own key schedule. In the method taught in Wood (US 5003596), a unique key schedule is created every time the disclosed block encryption process is executed (see reference number 38 in Fig. 2). Therefore, in the combined block encryption method of Wood (US 5003596) and Colvin, Sr (US 5841872) (the method of Wood (US 5003596) implemented using OOP), every time a new encryption key object is instantiated, a unique key table is created for the created encryption object.

As per claim 16, the claimed invention limits claim 5 so the object's key schedule is initialized using the random session key. This is disclosed in Fig. 2 of Wood (US 5003596)

where a unique key table is created from an initializing vector (also see column 9, lines 7-35). As mentioned is regards to claim 5, the examiner equates the initializing vector in the method taught in Wood (US 5003596) with the random session key in the claimed invention.

As per claim 19, the claimed invention limits claim 2 so the encrypting step uses a substitution array where the transposition of elements in the array is dependent upon an element of a key. Put another way, claim 19 teaches a keyed substitution array in the encrypting step.

The method of encrypting taught in Wood (US 5003596) also uses a keyed substitution array where the transposition of elements in the array depends upon the plaintext, ciphertext, and mask values (column 4, lines 6-11). The mask values in the method of Wood (US 5003596) act essentially as a key to manipulate the transposition of elements in a substitution array during encryption (see reference number 132 in Fig. 8 and also see Fig. 11 in Wood (US 5003596)).

As per claim 18, the claimed invention limits claim 5 so a keyed transposition of ciphertext blocks is performed after the encryption step. Put another way, claim 18 teaches a keyed permutation after the encrypting step.

The method of encrypting taught in Wood (US 5003596) also uses a keyed permutation where the transposition of elements in the array depends upon the plaintext, ciphertext, and mask values (column 4, lines 6-11). The mask values in the method of Wood (US 5003596) act essentially as a key to manipulate the transposition of elements in a permutation. Since the keyed permutation in Wood (US 5003596) can be the last step of the encryption process, Wood (US 5003596) discloses an encryption process followed by a keyed permutation. The examiner

further notes that scrambling ciphertext using a scrambling key is well known in the art of cryptography and is equivalent to the keyed permutation in claim 18.

As per claim 30, the claimed invention contains the same limitations as previously rejected claim 4 and is rejected for the same reasons.

As per claims 31 and 32, the claimed inventions contain the same limitations as previously rejected claim 5 and are rejected for the same reasons.

As per claim 34, the claimed invention contains the same limitations as previously rejected claim 19 and is rejected for the same reasons.

8. Claims 6, 7, 13, 14, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (US 5003596) in view of Colvin, Sr (US 5841872) and in further view of official notice.

As per claim 6, the claimed invention limits claim 5 so the random session key is created using a random number. The method disclosed in Wood (US 5003596) refers to an "initializing vector" but never explicitly discloses using a random number to create the initialization vector. Official notice is taken that it is well known in the art to create an initializing vector using a random number.

As per claim 7, the claimed invention limits claim 6 so a new random number is generated each time the block cipher encryption process is executed. In the combined method of Wood (US 5003596) and Colvin, Sr (US 5841872), one skilled in the art of object oriented programming would recognize a constructor of an encryption object would be called every time the object is instantiated. Therefore, official notice is taken that every time the encryption method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) is executed, a new random

number would be selected upon the object key's instantiation to seed a new set of encryption keys.

As per claim 13, the claimed invention limits claim 5 so the initial random session key is generated by using a rand() function call and seeding the rand() call using the time clock in a computer. The method taught in Wood (US 5003596) and Colvin, Sr (US 5841872) does not teach a specific way of generating the initializing vector. Official notice is taken that using an industry standard rand() function seeded by a computer clock is a well known method in the art of OOP for generating a pseudo-random number such as the initial random session value in the claimed invention.

As per claim 14, the claimed invention limits claim 5 so the random session key is modified by adding an offset to each byte in the current random session key. The method taught in Wood (US 5003596) and Colvin, Sr (US 5841872) teaches selecting a modified encryption key by choosing a new key from a derived key table based on the current state of plaintext, ciphertext, and mask values; however Wood (US 5003596) does not teach a method of selecting a modified encryption key by modifying an initializing vector in the manner described in claim 14.

Official notice is taken that it is well known to modify a current value by adding an offset to every byte in the value. Therefore, one of ordinary skill in the art at the time of the invention would know how to modify the initializing vector in the method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) using byte offsets so a new encryption key is derived from a modified initialization vector instead of from the current state of plaintext, ciphertext, and mask values.

As per claim 20, the claimed invention limits claim 19 so the position provided by an element of the key is bounded by the size of the substitution array. As discussed in regards to claim 19, the method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) teaches a keyed substitution array, but does not bound the element position provided by the array by the size of the array itself. Official notice is taken that a large substitution array can provide a larger number of element positions than a small substitution array. In other words, a 2-by-2 substitution array will not be able to provide as many key positions as a 10-by-10 array.

9. Claims 10, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (US 5003596) in view of Colvin, Sr (US 5841872) and in further view of Adams et al (US 5949884).

As per claim 10, the claimed invention limits claim 1 so the object key is dynamic and modification of the object key uses a hashing function. In the discussion of claims 3 and 4, it was shown the method disclosed by Wood (US 5003596) and Colvin, Sr (US 5841872) teaches a dynamic encryption object key, but the method of Wood (US 5003596) and Colvin, Sr (US 5841872) does not teach modifying the key using a hashing function.

Claims 17 and 18 in Adams et al (US 5949884) disclose a block encryption method where an original encryption key is divided into two or more sub-keys of equal length; each of the sub-keys is processed using a hash function to generate modified encryption keys (called "intermediate keys" in claim 18 of Adams et al (US 5949884)). Therefore, Adams et al (US 5949884) teach a method of creating a key schedule using hash functions since hash functions offer a fast and efficient method of creating a key schedule (column 2, lines 18-20, lines 53-55, and lines 63-67).

Since an encryption key in the method of Wood (US 5003596) and Colvin, Sr (US 5841872) is modified using an initializing vector and a key schedule, it would have been obvious to one of ordinary skill in the art at the time of the invention to generate the key schedule in the method of Wood (US 5003596) and Colvin, Sr (US 5841872) using hash functions, as taught in Adams et al (US 5949884), since Adams et al (US 5949884) teach hash functions are a fast and efficient tool for creating a modified key schedule.

As per claim 11, the claimed invention limits claim 1 so the object key is dynamic and includes at least two sub-object keys each with its own modification method. The block encryption method disclosed by Wood (US 5003596) and Colvin, Sr (US 5841872) does not teach using at least two sub-object keys each with its own modification method. As discussed in regards to claim 10, the method taught in Adams et al (US 5949884) discloses using at least two sub-keys each modified by a respective hash function (claims 17 and 18).

As per claim 15, the claimed invention limits claim 5 so the random session key is modified using a hash function. The method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) does not disclose hashing the initializing vector.

As mentioned previously, Adams et al (US 5949884) teach hashing an encryption key to generate a key schedule. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to hash an initializing vector to generate a key schedule used in the encryption method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) (where the initializing vector is tantamount to the "random session key" in the claimed invention) since Adams et al (US 5949884) teaches key schedule generation using hash functions is a fast and efficient method of generating a key schedule.

10. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (US 5003596) in view of Colvin, Sr (US 5841872) and in further view of Adams et al (US 5949884) and official notice.

As per claim 12, the claimed invention limits claim 5 so the object key includes at least two sub-keys and the random session key operations are performed using only one of the sub-keys. Wood (US 5003596) and Colvin, Sr (US 5841872) fully disclose claim 5 but do not teach using more than one sub-key.

As mentioned in regards to claims 10, 11, and 15, Adams et al (US 5949884) teach using more than one sub-key to generate key schedules. Official notice is taken that only one key schedule is needed to implement the block encryption method taught by Wood (US 5003596) and Colvin, Sr (US 5841872), and consequently the initializing vector would only need to be associated with a single sub-key.

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to generate the key schedule in the encryption method taught by Wood (US 5003596) and Colvin, Sr (US 5841872) using one of the sub-keys taught in Adams et al (US 5949884), since Adams et al (US 5949884) teaches a fast and efficient method of generating key schedules.

11. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (US 5003596) in view of Colvin, Sr (US 5841872) and in further view of Campbell, Jr (US 4369332).

As per claim 17, the claimed invention limits claim 2 so the plaintext is padded to be divisible by the block length. The method taught by Wood (US 5003596) and Colvin, Sr (US

5841872) fully discloses the limitations in claim 2, but does not teach padding (or salting) plaintext blocks to make them a fixed length.

The examiner notes this is common practice in the art of block encryption systems and the Campbell, Jr (US 4369332) reference is one of many references that teach the limitation in claim 17 (see column 4, lines 55-62 of Campbell, Jr (US 4369332)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to pad plaintext blocks to make them a fixed length, as taught in Campbell, Jr (US 4369332), in the block encryption method taught by Wood (US 5003596) and Colvin, Sr (US 5841872), since it is common practice in the art of block encryption systems to pad or salt plaintext blocks.

Allowable Subject Matter

12. Claims 9 and 21-24 are allowed.

As per claim 9, a method of modifying an object key is disclosed comprising specific rotations, multiplications, transpositions, and additions that are repeated for a fixed number of times. Although each step in the key modification is known separately, the examiner was not able to find in a single reference or a combination of references the specific sequence of operations disclosed in claim 9.

As per claim 21, a method of block cipher encryption is disclosed comprising repeated substitutions using the output from a transpositioning transverse array whose elements contain unique numbers; the outputs are summed and rotated in a sliding window and modulo-2 added to an element of a key, then repeated substitutions using the transpositioning transverse array are applied again. A final scrambling step is performed at the end of each round of encryption, where a specific number of rounds is disclosed in the encryption method.

The examiner was not able to find in a single reference or a combination of references that teach the specific sequence of operations disclosed in claim 21.

As per claims 22-24, the claimed inventions are allowed since they depend on allowed claim 21.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kaufman et al (US 5764772)

Shanton (US 5369702)

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steve Kabakoff whose telephone number is (703) 306-4153. The examiner can normally be reached on 8:30am to 6:00pm except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 305-9051 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

SK
SEK
March 9, 2000

TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700